BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered). Please AMEND claims 16, 19, 22, 24 and 26 in accordance with the following:

1. (previously presented) An electronic data storage apparatus for storing electronic documents included in a group of electronic data storage apparatuses including a main electronic data storage apparatus, said electronic data storage apparatus comprising:

a key management unit managing an individual key unique to said electronic data storage apparatus to which said management unit belongs, and a common key shared with other electronic data storage apparatuses of the group, selecting the individual key when performing an encryption process on an electronic document stored in said electronic data storage apparatus to which said management unit belongs, and selecting the common key when performing the encryption process or when verifying the electronic document transmitted to or received from another electronic data storage apparatus; and

an encryption unit performing the encryption process using the key selected by said key management unit, and

wherein said individual key is generated and distributed to said electronic data storage apparatus by said main electronic data storage.

2. (previously presented) The apparatus according to claim 1, wherein said key management unit manages a group key as the common key to be shared in said group.

3. (previously presented) The apparatus according to claim 1, wherein:

said encryption unit of said main electronic data storage apparatus generates an individual key of each electronic data storage apparatus in the group using an individual key of the apparatus to which said management unit belongs; and

said generated individual key is distributed to each electronic data storage apparatus belonging to the group.

4. (previously presented) The apparatus according to claim 2, wherein:

said encryption unit of said main electronic data storage apparatus generates a group key to be shared in the group using an individual key of the apparatus to which said management unit belongs; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

5. (previously presented) The apparatus according to claim 2, wherein:

said encryption unit of said main electronic data storage apparatus generates a group key to be shared in the group with a key preliminarily assigned as the individual key to said main electronic data storage apparatus associated with a new key externally specified; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

6. (previously presented) The apparatus according to claim 2, wherein:

an electronic data storage and management apparatus for managing respective main electronic data storage apparatuses in a plurality of groups exists;

said encryption unit of said electronic data storage and management apparatus generates an individual key of each of said main electronic data storage apparatuses using an individual key of the apparatus to which said management unit belongs; and

said generated individual key is distributed to each of said main electronic data storage apparatuses.

7. (previously presented) The apparatus according to claim 2, wherein said key management unit manages, in addition to said group key as the common key, a public key for use in transmitting the electronic document to and receiving the electronic document from an electronic data storage apparatus belonging to a group different from a group of the electronic data storage apparatus to which said management unit belongs.

8. (original) The apparatus according to claim 1, wherein said individual key is preliminarily assigned to each electronic data storage apparatus before use of the apparatus.

9. (previously presented) The apparatus according to claim 1, wherein:

said encryption unit generates the individual key with a key preliminarily set before use

of the apparatus to which said management unit belongs with a new externally specified key; and

said key management unit manages the generated Individual key.

10. (previously presented) The apparatus according to claim 1, wherein said key management unit manages, in addition to the individual key and the common key, a master key to be shared by all electronic data storage apparatuses.

11. (cancelled)

12. (previously presented) The apparatus according to claim 10, wherein:

said encryption unit of said main electronic data storage apparatus generates a group key as the common key by encrypting information identifying the group using the master key; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

13. (previously presented) The apparatus according to claim 1, wherein:

a hierarchical structure of electronic data storage apparatuses is designed as having the group of a plurality of electronic data storage apparatuses as one hierarchical level; and

said key management unit manages a group key as the common key depending on the hierarchical level of the group containing the electronic data storage apparatus to which said management unit belongs.

14. (previously amended) The apparatus according to claim 13, wherein:

in the hierarchical structure of the electronic data storage apparatuses, an electronic data storage and management apparatus for managing electronic data storage apparatuses in a lower order group exists in a group at one level higher than the lower order group;

said encryption unit of said electronic data storage and management apparatus generates a group key for the lower order group using the individual key of the apparatus to which said management unit belongs; and

said generated group key is distributed to the electronic data storage apparatuses in the group at one level lower.

15. (previously presented) A method of managing electronic documents in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, the group including said electronic data storage apparatus and a main electronic data storage apparatus, the method comprising:

re-encrypting, by a first electronic data storage apparatus in one hierarchical level of the hierarchical structure, a document encrypted using an individual key which is unique to and stored in the apparatus, using a higher order group key corresponding to the hierarchical level, and transmitting the re-encrypted document to an electronic data storage and management apparatus for managing the electronic data storage apparatuses in a group at one hierarchical level lower;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, the received document using the higher order group key, re-encrypting the received document using the lower order group key corresponding to one hierarchical level lower if the received documents is correct as a result of the verification, and transmitting the received document to a second electronic data storage apparatus in the group at one level lower; and

verifying, by the second electronic data storage apparatus, the received documents using the lower order group key, re-encrypting the received document using an individual key unique to the second electronic data storage apparatus if the electronic document is correct as a result of the verification, and storing the re-encrypted receiveddocument, and

wherein said individual key is generated and distributed by said main electronic data storage apparatus.

16. (currently amended) A method of managing electronic documents in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, the group including said electronic data storage apparatus and a main electronic data storage apparatus, the method comprising:

re-encrypting, by a first electronic data storage apparatus in one hierarchical level of the hierarchical structure, a document encrypted using an individual key which is unique to and stored in the first electronic data storage apparatus, using a lower order group key corresponding to the hierarchical level, and transmitting the re-encrypted document to a lower

order group electronic data storage and management apparatus for managing the electronic data storage apparatuses in the group;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, the received document using the lower order group key, re-encrypting the received ~~data~~ document using the higher order group key corresponding to one hierarchical level higher if the electronic document is correct as a result of the verification, and transmitting the document to a receiving electronic data storage apparatus in the group at one level higher;

verifying, by the receiving second electronic data storage apparatus, the received document using the higher order group key, re-encrypting the received document using an individual key unique to the second electronic data storage apparatus if the electronic document is correct as a result of the verification, and storing the re-encrypted received document, and

wherein said individual key is generated and distributed by said main electronic data storage apparatus.

17. (previously presented) A method of processing electronic documents, comprising:

storing in a storage unit an individual key unique to an electronic data storage apparatus for storing an electronic document and a common key shared with another electronic data storage apparatus;

selecting the common key stored in the storage unit as a key to be used when communicating the electronic document;

selecting the individual key to be used when performing an encryption process on the document to be stored in said electronic data storage apparatus; and

performing the communication process or encryption process using the selected key, and

wherein said individual key is generated and distributed to said electronic data storage apparatus by a main electronic data storage apparatus in a group of data storage apparatuses including said data storage apparatus.

18. (previously presented) The method according to claim 17, wherein;

said electronic data storage apparatus stores as the common key a group key shared in one group;

re-encrypting, by a first electronic data storage apparatus, an electronic document, encrypted using the individual key and stored in the first electronic data storage apparatus, using the group key, and transmitting the document to a second electronic data storage apparatus; and

verifying by the second electronic data storage apparatus, the received electronic document using the group key, re-encrypting the received electronic document using the individual key when the electronic document is correct according to the result of the verification, and storing the re-encrypted received document.

19. (previously presented) The method according to claim 17, wherein;

said electronic data storage apparatus belonging to one group stores as the common key a public key of an electronic data storage apparatus belonging to another group;

re-encrypting by a first electronic data storage apparatus, the electronic document, encrypted using individual key and stored in the first electronic data storage apparatus using the public key and transmitting ~~data~~ document to a second electronic data storage apparatus; and

verifying by the second electronic data storage apparatus the received electronic document using a private key which is a pair member with the public key, re-encrypting the received electronic document using the individual key when the electronic document is correct according to the result of the verification, and storing the re-encrypted received document.

20. (cancelled)

21. (cancelled)

22. (previously presented) An electronic data storage apparatus for storing electronic documents, comprising:

key management means for managing an individual key unique to an electronic ~~document~~ data storage apparatus to which said key management means belongs, and a common key shared with other electronic data storage apparatuses, selecting the individual key when performing an encryption process on the electronic document stored in the electronic data storage apparatus to which said means belongs, and selecting the common key when performing an encryption process or when verifying the electronic document transmitted to or received from another electronic data storage apparatus; and

encryption means for performing the encryption process using the key selected by said

key management unit, and

wherein said individual key is generated and distributed to said electronic data storage apparatus by a main electronic data storage apparatus in a group of data storage apparatuses including said data storage apparatus.

23. (previously presented) A computer-readable storage medium for storing a program which directs a computer to process electronic documents, comprising:

storing in a storage unit an individual key unique to an electronic data storage apparatus for storing an electronic document and a common key shared with another electronic data storage apparatus;

selecting the common key stored in the storage unit as a key to be used when communicating the electronic document;

selecting the individual key as a key to be used when performing an encryption process on the document to be stored in the electronic data storage apparatus; and

performing the communication process or the encryption process using the selected key, and

wherein said individual key is generated and distributed to said electronic data storage apparatus by a main electronic data storage apparatus in a group of data storage apparatuses including said data storage apparatus.

24. (previously presented) A method of ~~data~~ document transmission for a local environment and a global environment, comprising:

storing a local encryption key for the local environment locally and storing a global key for the global environment;

receiving a document to be transmitted along with an environment indicator indicating the environment of the document transmission;

selecting one of the local and global encryption keys responsive to the indicator;

encrypting the document with the selected one of the keys; and

transmitting the encrypted ~~data~~document, and

wherein the local key is used for data storage in a local data storage unit only by a local data storage system that stores the local key.

25. (previously presented) A method as recited in claim 24, wherein the local environment comprises a local area network, the global environment comprises the internet, and

the indicator is an address of the document transmission where a local area address indicates the local environment.

26. (previously presented) A method as recited in claim 25, wherein the method is performed by a data storage apparatus ~~data~~ document transmission, the ~~data~~ document transmission comprising a transmission to a data storage device having a device address within the data storage apparatus, said storing comprises storing a data storage device encryption key, and said selecting comprises selecting the device encryption key when the transmission is to the storage device.